Before the
Federal Communications Commission
Washington, D.C.

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Sarah K. Leggin
Director, Regulatory Affairs

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

December 10, 2021

TABLE OF CONTENTS

Before the
Federal Communications Commission
Washington, D.C.

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

COMMENTS OF CTIA

CTIA[1] respectfully submits these comments on the Federal Communications Commission's ("FCC" or "Commission") Further Notice of Proposed Rulemaking ("FNPRM") in the above-referenced proceedings.[2] CTIA and its member companies share the Commission's priority to protect consumers from illegal robocalls from overseas and welcome this opportunity to provide input on the Commission's efforts to further this goal.

I. INTRODUCTION AND SUMMARY.

CTIA and its member companies are dedicated partners in the Commission's efforts to protect consumers from illegal and unwanted robocalls, particularly those originating abroad. CTIA's member companies support the Commission's recent actions to give voice providers

[1] CTIA – The Wireless Association® ("CTIA") (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Fifth Further Notice of Proposed Rulemaking and Fourth Further Notice of Proposed Rulemaking, FCC 21-105 (Oct. 1, 2021) ("*FNPRM*").

more tools and resources to protect consumers,[3] and they have been implementing STIR/SHAKEN, deploying innovative call-blocking tools, and bolstering their robust robocall mitigation programs, among many other efforts domestically. Collectively, these efforts are providing a new level of protection for consumers from illegal and unwanted robocalls, including those originated abroad, while also safeguarding legitimate calls.

With this FNPRM, the Commission has rightly focused on taking further action to shut down illegal and unwanted robocalls that originate overseas, which is a goal that the wireless industry shares. CTIA and its member companies have been hard at work educating their foreign provider partners and encouraging them to implement robocall mitigation programs and to register in the Commission's Robocall Mitigation Database ("RMD"), and appreciate the Commission's suspension of the foreign provider prohibition as these and other efforts continue.[4] These efforts, combined with the Commission's aggressive enforcement actions

[3] *See, e.g.*, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd. 7614, ¶ 3 (2020) ("[E]stablishing a safe harbor from liability under the Communications Act and the Commission's rules for the unintended or inadvertent blocking of wanted calls, so long as such action is based upon reasonable analytics indicating that such calls were unwanted and therefore should be blocked."); *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Fourth Report and Order, 35 FCC Rcd. 15221, ¶ 39 (2020) ("[E]xpand[ing] the safe harbor based on reasonable analytics to cover network-based blocking if the network-based blocking incorporates caller ID authentication information where available and otherwise meets the requirements we adopted both in the *Call Blocking Order and Further Notice* and elsewhere in this *Order*.") ("*Fourth Report & Order*"); *Protecting Consumers from One-Ring Scams*, CG Docket No. 20-93, Report and Order, 35 FCC Rcd. 14236, ¶ 7 (2020) ("[W]e expressly enable voice service providers to block all calls from telephone numbers that are highly likely to be associated with one-ring scams, consistent with section 12(b)(4) of the TRACED Act.").

[4] *See FNPRM* ¶ 106 ("In light of the unique difficulties foreign service providers may face in timely registering with the Commission's new Robocall Mitigation Database, the fact that the foreign provider prohibition can be evaded by transmitting traffic via one or more foreign intermediate providers, and in order to avoid the potential disruption associated with such delays while permitting the Commission to explore these potentially more effective measures, we

against bad actors and certain gateway providers facilitating illegal voice traffic from overseas are critical steps in the fight against illegal robocalls originating from foreign providers.[5]

To promote further progress in protecting U.S. networks from illegal and unwanted robocalls, the Commission's focus moving forward in this proceeding should be on promoting more widespread implementation of robust robocall mitigation programs, including by all intermediate providers, as well as increased education and collaboration with foreign counterparts. The Commission should also continue to leverage existing tools that have proven effective in helping protect U.S. networks from illegal foreign-originated robocalls, while maintaining the careful balance between fighting illegal robocalls and protecting legitimate calls under the robocall abatement framework already deployed. This should include continuing enforcement against bad actor providers that are not mitigating illegal foreign robocalls and requiring updates to those providers' robocall mitigation programs that are deemed insufficient, as well as encouraging ongoing participation by all providers in traceback, know-your-customer, call blocking, call authentication, and other efforts to protect consumers.

---

conclude that the public interest will be served by not enforcing the foreign provider prohibition during the pendency of this proceeding.").

[5] *See e.g.*, Press Release, FCC, *FCC Demands Three More Companies Immediately Stop Facilitating Illegal Robocall Campaigns* (Oct. 21, 2021), https://docs.fcc.gov/public/attachments/DOC-376789A1.pdf (discussing the issuance of three cease and desist letters to voice providers, and demanding they "immediately cease originating illegal robocall campaigns on their networks, many of which originated overseas, and report to the Commission the concrete steps they are implementing to prevent a recurrence of these operations."); *see also* Letter from the Federal Communications Commission and Federal Trade Commission, to Craig Denson, CEO, PTGi International Carrier Services, Inc. (May 20, 2020), https://www.ftc.gov/system/files/warning-letters/covid-19-letter_to_ptgi_carrier_services.pdf (demanding that the voice provider cease routing illegal robocall traffic immediately, and noting that the company was "a gateway voice provider for apparently fraudulent COVID-19 robocalls originating from a Germany-based wholesale provider, which [the] company refused to identify by name.") ("*PTGi Enforcement Letter*").

By taking targeted action to promote robocall mitigation by intermediate providers, enforce against bad actors facilitating illegal traffic, and allow gateway providers to leverage existing tools and frameworks to protect consumers, the Commission can make meaningful progress in its efforts to protect U.S. networks from robocalls originated abroad.

II. THE WIRELESS INDUSTRY CONTINUES TO AGGRESSIVELY FIGHT FOREIGN-ORIGINATED ILLEGAL ROBOCALLS ACROSS MULTIPLE FRONTS.

CTIA's member companies and their partners across the voice ecosystem continue to work on multiple fronts to ensure that their overseas partners are taking effective and appropriate measures to mitigate foreign-originated illegal robocalls. Since the Commission established the foreign provider prohibition in 2020,[6] U.S. providers have worked diligently to educate their foreign counterparts about call authentication, robocall mitigation, and registration expectations. This outreach includes individual providers directly engaging with their foreign counterparts, as well as efforts to increase awareness of these changes through existing industry bodies such as the GSMA, the Communications Fraud Control Association, and the M3AAWG. This work is showing results. While CTIA applauds the Commission's decision to hold in abeyance the foreign provider prohibition, given the operational and call completion issues that it raised,[7] even

[6] *See* 47 C.F.R. § 64.6305(c); *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd. 1859, ¶ 90 (2020) ("Thus, foreign voice service providers that use NANP numbers that pertain to the United States to send voice traffic to residential and business subscribers in the United States must follow the same certification requirements as domestic voice service providers in order to be listed in the database. Because we prohibit domestic intermediate providers and terminating voice service providers from accepting traffic from foreign voice service providers that use NANP numbers that pertain to the United States and are not listed in the database, we create a strong incentive for such foreign voice service providers to file certifications.") ("*Second Report & Order*").

[7] *See FNPRM* ¶ 106. CTIA appreciates the Commission's recognition that further review of the rules is needed so that gateway providers block only illegal robocalls and not legitimate international calls; *see also* Letter from Scott Bergmann, Senior Vice President, Regulatory Affairs, CTIA, to Marlene H. Dortch, Secretary, FCC, at 2 (Apr. 12, 2021),

absent enforcement of the prohibition, many foreign voice service providers have implemented robocall mitigation plans and have continued to register in the FCC's RMD. Indeed, based on the education and outreach efforts of CTIA members, 99 percent of AT&T's international traffic comes from carriers registered in the RMD;[8] T-Mobile reports that it now receives all of its inbound international traffic from providers registered in the RMD; and Verizon likewise has confirmed that over 99 percent of traffic received from foreign service providers is now from ones registered in the RMD. And beyond RMD registration, domestic voice service providers continue to modify their interconnection contracts with foreign providers to focus on the need to mitigate illegal robocall traffic.

In addition to direct engagement with their foreign counterparts, CTIA members—including those that act as gateway providers—take additional steps to protect consumers from illegal robocalls originating from abroad. These efforts include active participation in traceback efforts that have assisted in federal and state enforcement actions against providers facilitating illegal robocall traffic, including from overseas;[9] blocking of illegal and unwanted robocalls,

---

https://ecfsapi.fcc.gov/file/1041266774641/210412%20FINAL%20CTIA%20Ex%20Parte%20re%20Foreign%20Provider%20Prohibition%20PFR.pdf (encouraging the Commission to issue a further notice to address the issues raised by the Foreign Provider Prohibition, including clarifying the scope and implementation of the new rule to ensure the appropriate providers are taking steps to help mitigate robocalls).

[8] *See* Letter from Linda S. Vandeloop, Assistant Vice President, Federal Regulatory, AT&T Services, Inc., to Marlene H. Dortch, Secretary, FCC, at 1 (Sept. 23, 2021), https://ecfsapi.fcc.gov/file/109241616012712/ATT%20WC%20Docket%2017-97%20CG%20Docket%2017-59.pdf.

[9] *See* Press Release, FCC, *FCC Designates Robocall Traceback Manager*, (July 27, 2020) https://docs.fcc.gov/public/attachments/DOC-365751A1.pdf (quoting Rosemary Harold, Chief of the Enforcement Bureau, as stating that the "Industry Traceback Group has been and will continue to be a vital partner in our pursuit of unlawful robocallers."); *see also* Complaint at 13-15, *United States of America v. Palumbo, et al.*, 448 F. Supp. 3d 257 (E.D.N.Y. 2020) (CV 20-473) (discussing industry efforts to traceback illegal robocalls to TollFreeDeals, which facilitated hundreds of millions of such robocalls); *see also*, Letter from the Federal Trade Commission and the Federal Communications Commission, to Jonathan Spalter, President and

both through consumer-facing tools and at the network level, encouraged by safe harbors;[10] and other tools and strategies to protect consumers, including implementing STIR/SHAKEN and other call authentication approaches, as well as know-your-customer (KYC) best practices, among others.

III. THE COMMISSION SHOULD PROMOTE ROBOCALL MITIGATION BY ALL PROVIDERS AND CONDUCT OUTREACH TO FOREIGN COUNTERPARTS TO PROTECT CONSUMERS FROM ILLEGAL ROBOCALLS ORIGINATED ABROAD.

In addition to the significant work already underway to thwart foreign-originated illegal robocalls, the Commission can take targeted steps to further protect U.S. consumers from illegal robocalls, including those from overseas. By clarifying that intermediate providers, including foreign intermediate providers, are expected to implement robocall mitigation programs and by conducting outreach to foreign regulators and other stakeholders to promote RMD expectations, the Commission can make its RMD more effective in helping providers protect U.S. networks from robocalls originated abroad.

First, to further protect consumers from foreign originated robocalls, the Commission should continue to promote RMD certifications and require *all* operators—including intermediate providers—to implement robocall mitigation programs. As noted above, industry

---

CEO, USTelecom, (May 20, 2020), https://www.ftc.gov/system/files/attachments/press-releases/ftc-fcc-send-joint-letters-additional-voip-providers-warning-against-routing-transmitting-illegal/fcc-ftc-letter_to_ustelecom-5-20-20.pdf (expressing gratitude to the Industry Traceback Group's "prompt response to identify and mitigate fraudulent robocalls that are taking advantage of the national health crisis related to the Novel Coronavirus Disease (COVID-19).").

[10] *See Call Blocking Tools Available to Consumers: Second Report on Call Blocking*, CG Docket No. 17-59, Report, DA 21-772, ¶ 3 (June 29, 2021) ("[M]any voice service providers and third-party analytics companies offer improved call blocking services to their customers to protect them from illegal and unwanted calls. Voice service providers and third-party analytics companies use new data continually to update their analyses to detect robocalls; they report offering consumers more blocking tools and blocking more calls.").

stakeholders have made significant strides in encouraging their foreign partners to implement robocall mitigation programs so they can register in the RMD, and many report that all, or nearly all, of their foreign partners that originate traffic have now registered, even absent enforcement of the foreign provider prohibition.

To further enhance the effectiveness of the RMD in protecting against foreign originated robocalls, the Commission should clarify that foreign intermediate providers must also implement robocall mitigation programs and certify to such in the RMD in order for their traffic to be accepted by domestic intermediate and voice service providers.[11] Promoting robocall mitigation by intermediate providers will promote use of these techniques by all entities in the call path and in turn help protect U.S. networks from illegal traffic. CTIA continues to encourage the Commission to allow sufficient time for additional foreign registrations to occur prior to implementing and enforcing the foreign provider prohibition.[12]

The Commission should also take the opportunity to require domestic intermediate providers to implement robocall mitigation programs and certify to such in the RMD as well. This will help mitigate uncertainty regarding certification requirements, and will help clarify that each provider needs to help establish the chain of trust across the voice ecosystem.[13]

---

[11] As the Commission notes in the *FNPRM*, "[b]y its terms, [the foreign provider prohibition] does not require U.S.-based providers to reject foreign-originated traffic carrying U.S. NANP numbers that is received by a U.S. provider directly from a foreign intermediate provider—at present, the prohibition only applies to traffic received directly from the originating foreign provider." *FNPRM* ¶ 104. Applying the foreign provider prohibition to intermediate providers would effectively require providers to implement robocall mitigation programs.

[12] *Call Authentication Trust Anchor*, Petition for Partial Reconsideration of CTIA, WC Docket No. 17-97 (filed Dec. 17, 2020).

[13] The Commission should also allow sufficient time for domestic certifications to robocall mitigation occur before enforcing the ban on accepting traffic from non-certified intermediate providers as well.

Second, to help encourage foreign providers to engage in robocall abatement, the Commission should also educate its foreign government counterparts on efforts to protect consumers from robocalls and encourage regulators abroad to promote foreign provider participation in robocall mitigation and the Commission's RMD. Such education should include the importance of supporting cooperation on traceback requests, consistent with the Commission's existing robocall framework. The Commission should update the public and industry stakeholders on its efforts to educate foreign stakeholders and the status of their engagement. Given that domestic voice service providers can only rely on the registrations and certifications in the RMD when accepting voice traffic, such outreach by the Commission will be critical to achieving the agency's goals of increased certifications by foreign providers in the RMD prior to implementing the foreign provider prohibition.

IV. THE COMMMISSION'S EXISTING MITIGATION FRAMEWORKS PROVIDE POWERFUL TOOLS FOR GATEWAY PROVIDERS TO FURTHER PROTECT CONSUMERS FROM ILLEGAL ROBOCALLS FROM OVERSEAS.

CTIA and its member companies agree with the Commission's focus on protecting consumers from illegal robocalls entering the U.S., and providers are taking significant actions to achieve this goal, as discussed above. The Commission should continue to protect consumers through strong enforcement activity against bad actors and promotion of the many existing tools the Commission and industry have recently unleashed. This approach is preferable to imposing overly rigid requirements exclusively on gateway providers, which would upset the careful balance between fighting illegal robocalls and protecting legitimate calls that the existing robocall abatement framework strikes.

The Commission should continue to focus on stopping bad actors originating and facilitating illegal robocalls from abroad. Specifically, for providers that are suspected to be

facilitating illegal traffic, the Commission can leverage its current requirement on all U.S. providers, including gateway providers,[14] to effectively mitigate illegal traffic when notified by the Commission.[15] The Commission's framework for targeting and stopping suspected bad traffic through this tool specifically contemplates application to gateway providers.[16] Once notified by the Commission, gateway providers must first investigate the source of the suspected bad traffic and then "take steps to 'effectively mitigate illegal traffic within 48 hours.'"[17] These steps could include a range of actions from terminating a customer relationship to blocking illegal traffic, or other efforts to enhance existing their robocall abatement solutions.[18] Gateway providers must then inform both the Commission and the Traceback Consortium within fourteen days of the date of the letter of the steps they have taken to "implement effective measures" to prevent customers from using their network to make illegal calls.[19]

---

[14] *See Fourth Report & Order* at n.2 & ¶14 (explaining that the definition of "voice service provider" for the purposes of its affirmative obligations for voice service providers includes intermediate providers); *see also FNPRM* ¶ 21 ("[T]he Commission, in the *Fourth Call Blocking Order*, established three affirmative obligations that apply to voice service providers (including intermediate providers).").

[15] 47 C.F.R. § 64.1200(n)(2) ("A voice service provider must . . . [t]ake steps to effectively mitigate illegal traffic when it receives actual written notice of such traffic from the Commission through its Enforcement Bureau.").

[16] *See Fourth Report & Order* ¶ 23 ("We generally expect that the Enforcement Bureau will notify either the originating voice service provider that has a direct relationship to the caller or the intermediate provider that is the gateway onto the U.S. network.").

[17] *See e.g.* Letter from Rosemary C. Harold, Chief, Enforcement Bureau, FCC, to Christopher Ismail, CEO, Duratel LLC, at 1 (Oct. 21, 2021), https://docs.fcc.gov/public/attachments/DOC-376747A1.pdf (citing to 47 CFR § 64.1200(k)(4)) ("*Duratel Enforcement Letter*").

[18] *See Fourth Report & Order* ¶ 26. Importantly, the Commission has recognized that intermediate providers among others "have limited visibility into the actual source of the traffic" and accordingly, the Commission "do[es] not expect perfection in mitigation." *Id.* ¶ 30.

[19] *See Duratel Enforcement Letter*, p. 1.

In practice, this tool has already proven effective to target appropriate mitigation measures towards the gateway providers permitting illegal robocall traffic to enter the United States. For example, the Commission has issued cease and desist letters to multiple providers, including gateway providers, to stop illegal traffic.[20] This existing enforcement approach provides the Enforcement Bureau with important insight into illegal traffic mitigation measures that gateway providers are taking,[21] and in turn allows both the Commission and providers alike to nimbly respond—in real time—to complex illegal robocalling threats and evolving tactics by bad actors. The Commission, along with the Federal Trade Commission ("FTC") and state Attorneys General, should continue to pursue these targeted enforcement efforts, which demonstrate remarkable effectiveness in mitigating illegal robocalls, including those originating from overseas.[22]

In addition to continuing strong and targeted enforcement activity, the Commission should continue to allow gateway providers to take advantage of the various tools and resources that the Commission and industry have unleashed over the past several years to defend

[20] *See e.g.*, *See PTGi Enforcement Letter* (letter to gateway provider).

[21] *See e.g. Duratel Enforcement Letter*, p. 1 (demanding that the voice provider cease routing illegal robocall traffic immediately, and "inform the Commission and the Traceback Consortium within fourteen (14) days of the date of this letter (November 5, 2021) of the steps [the company has] taken to 'implement effective measures' to prevent customers from using [the company's] network to make illegal calls.").

[22] For example, the Federal Trade Commission reported that after initiating its enforcement action against Globex Telecom, and subsequently issuing more than thirty warning letters to VoIP providers, the agency saw a dramatic drop in Do Not Call ("DNC") complaints. Specifically, immediately after the Globex lawsuit, DNC complaints "dropped by a whopping 25%, compared to December 2018." Further, after the FTC's warning letters were issued to VoIP providers, "reports in February 2020 were more than 30% lower than the previous year. And March of 2020 had 53% fewer robocall reports than March of 2019." *See*, FTC Consumer Information Blog, *The FTC keeps attacking robocalls*, (Apr. 3, 2020), https://www.consumer.ftc.gov/blog/2020/04/ftc-keeps-attacking-robocalls?page=3.

consumers against bad actor illegal robocallers, including robust and flexible traceback, call blocking, know-your-customer, and call authentication approaches.

First, the Commission should promote gateway provider participation in traceback efforts under its current framework. As recent enforcement actions demonstrate, under the current traceback framework, industry efforts have been a key element in the Commission's efforts to crack down on bad actors and their partners that facilitate illegal robocalls.[23] Already, U.S. intermediate providers, including gateway providers, are required to "respond to traceback requests from the Commission, civil and criminal law enforcement, and the Consortium . . . [both] fully and timely."[24] The Commission should maintain its current approach for U.S. providers and avoid unnecessary changes to its existing processes and procedures, especially for one narrow segment of providers.[25] Specifically, mandating a 24-hour deadline for a full traceback request response by gateway providers is unnecessary as all providers that participate already work to respond as quickly as possible.[26]

---

[23] *See e.g.*, *In the Matter of John C. Spiller et al.*, Forfeiture Order, 36 FCC Rcd. 6225, ¶¶ 5, 9 (Mar. 18, 2021) (discussing the critical role of the Industry Traceback Group in identifying the source of the illegal robocalls originated by Spiller and Mears).

[24] *See Fourth Report & Order* ¶ 15; *see also FNPRM* ¶ 52 (noting the "general obligation, which requires that voice service providers (including intermediate providers) respond to traceback requests 'in a timely manner'").

[25] *FNPRM* ¶ 52 (proposing "to require gateway providers to respond fully to all traceback requests from the Commission, civil or criminal law enforcement, and the industry traceback consortium within 24 hours of receiving such a request"). Clarifying that intermediate providers should implement robocall mitigation programs and register in the RMD, as suggested above, will have a greater impact than by encouraging broader participation in traceback than imposing an unnecessary response timeframe, as all registrants in the RMD must "commit[] to respond fully and in a timely manner to all traceback requests." 47 C.F.R. § 64.6305(b)(2)(iii).

[26] *See* Industry Traceback Group, Combatting Illegal Robocalls, pp. 2 – 3, https://www.ustelecom.org/wp-content/uploads/2021/02/ITG-Report-Combatting-Illegal-Robocalls.pdf (last visited Dec.1, 2021) (noting that the average time for the ITG to complete an individual hop is now less than 24 hours and the average time for the ITG to complete a traceback is approximately 4 days, which is notable given that such tracebacks "usually rout[e]

Second, the Commission should maintain its permissive call-blocking framework, which has strengthened the ability of voice service providers to protect consumers. Balancing call completion with robocall abatement is critical, and the Commission's existing blocking framework—which permits but does not require blocking—best allows providers to efficiently target and stop unwanted and illegal calls, while ensuring that they can continue to deliver legitimate ones, especially emergency and public safety calls. The Commission should not deviate from this carefully crafted and long-standing approach for permissive blocking of illegal robocalls,[27] as doing so would upend the Commission's careful balance and would have serious call completion implications for legitimate calls that originate outside of the United States.[28] Rather, the Commission should work with gateway providers under the existing permissive model, and continue to encourage them to deploy more tools, including those aimed at blocking calls originating abroad when appropriate.

Third, the Commission should continue to allow all providers to deploy their KYC practices under the current flexible approach,[29] which "permit[s] [voice service providers] flexibility to determine what works best on their networks."[30] Providers, including both

---

through 4 or more, or sometimes as many as 9 or 10 service providers (or "hops") across the globe.").

[27] *FNPRM* ¶ 56 ("[W]e seek comment on several possible approaches to requiring gateway providers to block calls, particularly where those calls bear a U.S. number in the caller ID field.").

[28] *Id.* ¶ 106 (stating that the Commission would delay implementation of the foreign provider prohibition in order to "avoid the potential disruption" associated with its requirement to block traffic from certain providers).

[29] 47 C.F.R. § 64.1200(n)(3) ("A voice service provider must . . . [t]ake affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic.").

[30] *See Fourth Report & Order* ¶ 32.

intermediate and gateway providers, already implement robust KYC for their interconnection partners. And while each provider takes different approaches, as the Commission understands is necessary in light of differences in providers and call patterns,[31] gateway providers have a shared goal of ensuring trust in the voice ecosystem, particularly with their interconnection partners.

Given that providers already implement KYC, requiring prescriptive KYC practices—such as requiring gateway providers to confirm who has the right to use specific NANP numbers—is unnecessary, overly burdensome, and likely unworkable.[32] As the Commission acknowledges in the FNPRM, "gateway providers may not have a 'customer' to 'know' for the purpose of complying with a 'know your customer' requirement."[33] This dynamic is further complicated in the context of NANP numbering resources, whereby even if a gateway provider "knows" its interconnection partner, the same gateway provider often does not have direct relationship with the originating customer utilizing the NANP resources at issue. This reality generally inhibits the ability of any gateway provider to confirm that a foreign originator is authorized to use the particular U.S. number that purports to originate a call, rendering the Commission's KYC proposal unworkable.[34] As a result, the Commission should maintain its flexible approach to promoting gateway providers' KYC practices.

---

[31] *See id.* ¶ 34 ("Different call patterns may require different approaches, and methods that are appropriate for one voice service provider may not be the best for others. Voice service providers can comply in a number of ways, so long as they know their customers and take measures that have the effect of actually restricting the ability of new and renewing customers to originate illegal traffic.").

[32] *FNPRM* ¶ 80 ("[W]e propose and seek comment on requiring gateway providers to confirm that a foreign call originator is authorized to use a particular U.S. number that purports to originate the call.").

[33] *Id.*

[34] *See id.* ¶ 81. Such foreign originator could feasibly be two, three, or more hops away from the domestic gateway provider.

Fourth, the Commission should continue to allow flexibility in gateway providers' management of unauthenticated traffic originated abroad. Although the Commission proposes to "[r]equir[e] gateway providers to authenticate caller ID information for all unauthenticated foreign-originated SIP calls,"[35] gateway providers generally do not have access to information needed to authenticate traffic coming in from abroad or to determine whether a foreign call originator has the right to use a given U.S. number to make the call. The Commission already concluded that flexibility is important for intermediate providers to manage unauthenticated traffic when it originally declined to require gateway providers to authenticate foreign traffic last year,[36] acknowledging that gateway providers do not have a direct relationship with the foreign initiator of a call.[37] Further, STIR/SHAKEN is generally not mandated outside of the U.S., so even providers with a direct relationship are probably not partnering with a foreign provider that has implemented STIR/SHAKEN. While providers in industry standards bodies are focused on how to promote the use of call authentication with foreign partners, this work is in its nascent stages, and it would be premature for the Commission to adopt authentication requirements here. For these reasons, the Commission should maintain its flexible approach to allow gateway

[35] *Id.* ¶ 40.

[36] *See Second Report and Order* ¶ 140 ("[W]e require that an intermediate provider authenticate the caller ID information of a call that it receives with unauthenticated caller ID information that it will exchange with another intermediate provider or terminating voice service provider as a SIP call. However, a provider is relieved of this obligation if it (i) cooperatively participates with the industry traceback consortium and (ii) responds to all traceback requests it receives from the Commission, law enforcement, or the industry traceback consortium regarding calls for which it acts as an intermediate provider.").

[37] *See id.* ¶ 10 (noting that providers will use "uses a C-level attestation when it is the point of entry to the IP network for a call that originated elsewhere but has no relationship with the initiator of a call, such as when a provider is acting as an international gateway").

providers to determine whether attestation is appropriate for unauthenticated foreign originated calls.

Fifth, the Commission should continue to enable evolving consumer needs to drive contractual agreements among industry stakeholders. Consistent with NANC and industry recommendations relating to contractual terms, providers (including gateway providers) already consider their partners' reputation with regard to consumer protection and require their customers to adopt contractual provisions that help to mitigate illegal robocalls.[38] This diversity in contractual terms by a broad range of providers further enhances robocall mitigation efforts by ensuring that parties are contractually obligated to take affirmative measures to mitigate such traffic. Commission oversight of such private contractual arrangements as proposed in the FNPRM is therefore unnecessary and would ultimately be counterproductive.[39]

V. CONCLUSION.

CTIA appreciates the Commission's continued focus on protecting consumers from illegal robocalls from overseas, and the wireless industry remains dedicated to partnering with the Commission in this effort. CTIA supports targeted actions to help enhance robocall mitigation by all providers, and urges the Commission to leverage available tools and otherwise maintain its current approach to mitigating foreign-originated illegal robocalls—which combines strong and targeted enforcement activity with flexibility for providers to use a variety of tools in

[38] *See e.g.*, North American Numbering Council (NANC) Call Authentication Trust Anchor Working Group, *Best Practices for the Implementation of Call Authentication Frameworks*, pp. 14 – 16 (Sept. 24, 2020), https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf (recommending contractual solutions between domestic and international providers, that include the vetting of customers and the validation of telephone numbers used for the services offered.).

[39] *FNPRM* ¶ 87 ("We seek comment on whether . . . we should require gateway providers to adopt specific contractual provisions addressing robocall mitigation with foreign providers from which the gateway provider directly receives traffic carrying U.S. NANP numbers, and, in some cases, traffic from their foreign-end user customers. . . . ").

the Commission's deep toolbox to protect consumers from illegal and unwanted robocalls originated abroad.

Respectfully submitted,

/s/ Sarah K. Leggin
Sarah K. Leggin
Director, Regulatory Affairs

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs